UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

GARY HOLZ, JOEL GUAY, and GLORIA MONCRIEF, individually and on behalf of all others similarly situated, Plaintiffs, v. FRED HUTCHINSON CANCER CENTER, a Washington Nonprofit Corporation, Defendant.	No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Gary Holz, Joel Guay, and Gloria Moncrief (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, by and through their counsel, bring this Class Action Complaint against Defendant Fred Hutchinson Cancer Center d/b/a Fred Hutch ("Fred Hutch" or "Defendant") and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities and alleges, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs and Class Members were required to provide Defendant their confidential and sensitive information to obtain medical services. Defendant failed to maintain adequate security protocols in storing and/or transferring this information, and as a result,

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

cybercriminals were able to infiltrate Defendant's computer systems and steal Plaintiffs' and Class Members' highly sensitive personal information.

2. To make matters worse, the instant data breach is not Defendant's first data breach. Defendant was also hacked on March 25, 2022 when it "discovered suspicious activity associated with a single employee's business email account."[1] Defendant admitted that during that 2022 data breach, "an unauthorized individual accessed the account between March 25 and March 26, 2022" and was able to steal current and former patients' personal information.[2]

3. Despite this prior data breach, Defendant has *still* failed to provide adequate data security which resulted in yet another data breach. Specifically, on November 19, 2023, Defendant "detected unauthorized activity on our clinical network" and learned that cybercriminals were able to access Defendant's computer systems ("Data Breach") and, on information and belief, were able to exfiltrate current and former patient's personally identifiable information ("PII") and protected health information ("PHI") ("PII" and "PHI" or, collectively, "Personal Information").[3] Defendant also admits it believes that "the criminal group responsible [for the Data Breach] is outside the United States."[4]

4. Plaintiffs are victims of the Data Breach, having received a breach notice. Plaintiffs bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

II. JURISDICTION AND VENUE

---

[1] *See* Notice of Data Breach, CALIFORNIA ATTY GEN, https://oag.ca.gov/system/files/%28AD%20CM%2012M%29%20ELN-15938%20Fred%20Hutchinson%20CC.pdf (last visited December 27, 2023).
[2] *Id.*
[3] *See* FRED HUTCH, *Update on Data Security Incident* (Dec. 7, 2023) https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html (last visited December 27, 2023).
[4] *Id.*

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

5. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.[5]

6. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in Washington; it is registered with the Secretary of State in Washington as a Washington nonprofit corporation; it maintains its headquarters in Washington; and committed tortious acts in Washington.

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Defendant has the most significant contacts.

III. PARTIES

8. Plaintiff Gary Holz is an individual and a resident of King County, Washington.

9. Plaintiff Joel Guay is an individual and is a resident of King County, Washington.

10. Plaintiff Gloria Moncrief is an individual and a resident of Snohomish County, Washington.

11. Defendant, Fred Hutchinson Cancer Center, is a Washington Nonprofit Corporation with its principal place of business at 1100 Fairview Ave N, Seattle, Washington 98109.

IV. FACTUAL BACKGROUND

Defendant's Collection of Plaintiffs' and Class Members' Personal Information

12. In April 2022, Fred Hutchinson Cancer Center was created by way of a merger of Fred Hutchinson Cancer Research Center with the Seattle Cancer Care Alliance (SCCA). The

[5] Defendant submitted notice of the Data Breach to the Office of the California Attorney General indicating that at least one California resident was a victim of the Data Breach: https://oag.ca.gov/ecrime/databreach/reports/sb24-578365

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

result of unifying these research and patient care entities was the creation of a unified adult cancer research and care center that is clinically integrated with University of Washington (UW) Medicine and UW Medicine's cancer program. The purpose of this merger was to integrate scientific endeavors and clinical care to ensure patients have access to the most innovative care. As a result of the restructuring, Fred Hutch now serves as UW Medicine's cancer program.[6]

13. Fred Hutch is an independent organization that specializes in cancer care as well as cancer and infectious disease research.[7] It conducts research in more than 60 difference countries and employs roughly 5700 people.[8]

14. As part of its general business practices, Defendant stores large amounts of highly sensitive Personal Information about its current and former patients, including Plaintiffs and Class Members.

15. In collecting and maintaining Plaintiffs' and Class Members' Personal Information, Defendant agreed that it would safeguard their Personal Information in accordance with its internal policies and state law.

16. Under state law, entities like Defendant have duties to protect its current and former patients' Personal Information and to notify them about any data breaches.

17. Defendant knew of its duties under state law to implement adequate cyber security practices and policies. Indeed, Defendant made affirmative representations to Plaintiffs and Class Members that they would protect their Personal Information.

---

[6] *See Hutch News Stories: Fred Hutch and Seattle Cancer Care Alliance unite, reshape relationship with UW Medicine, Fred Hutch Cancer Center* (Apr. 1, 2022), https://www.fredhutch.org/en/news/center-news/2022/04/fred-hutch-scca-restructure.html (last visited December 27, 2023).

[7] *See About Us,* FRED HUTCH, https://www.fredhutch.org/en/about.html (last visited December 27, 2023).

[8] *Id*.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

18. Specifically, Fred Hutch's "Privacy Policy and Terms of Use," provides:

> Fred Hutch has a Privacy Policy that describes how we collect information from you or about you, why we collect this information, how we will use or disclose this information. In addition, Fred Hutch's Privacy Policy sets forth our general policies on information security."[9]

Defendant's Pattern of Negligence

19. As discussed above, Defendant's current Data Breach is not an isolated incident and is in fact a part of a pattern of Defendant's continued negligent data security practices.

20. The instant Data Breach is the second time that Defendant has experienced a serious data breach within the last couple of years.[10] Specifically, between March 25 and March 26, 2022, Defendant's data systems were hacked by an unknown and unauthorized individual.[11] This prior data breach also exposed the Personal Information of Defendant's patients.[12]

21. Clearly, Defendant has not learned from its recent mistakes and its negligence has caused yet another data breach to occur approximately one year later.

The Data Breach

22. On or about between December 6, 2023 and December 8, 2023, Defendant sent Plaintiffs and, on information and belief, Class Members, emails pertaining to the Data Breach and the threatening ransom emails that Class Members have been receiving from cybercriminals. Specifically, one variation of the email provided:

> Dear valued community,
>
> We're writing to alert all current and former patients (including former Seattle Cancer Care Alliance patients) that Fred Hutchinson Cancer Center recently experienced a cybersecurity incident. We took immediate action to contain the

---

[9] *See* FRED HUTCH, *Privacy Policy and Terms of Use*, https://www.fredhutch.org/en/util/terms-privacy.html (last visited December 27, 2023).
[10] *See Supra*, at Footnote No. 1.
[11] *Id.*
[12] *Id.*

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

impact, contacted federal law enforcement, engaged a leading forensic security firm, and proactively took our clinical network offline.

All Fred Hutch clinics are open and actively serving patients.

Our patients' health and safety is our top priority. Our forensic team is continuing to assess the data involved. We are working to complete the investigation as quickly as possible and will contact any individuals whose information was involved.

In the meantime, as a precautionary measure, we recommend you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that maintains the account. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to appropriate law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

It is also common for cyber criminals to send threatening spam messages and demand money. If you receive suspicious or threatening phone calls or emails, report these messages to the FBI's Internet Crime Complaint Center at ic3.gov. Then block the sender, delete the message and do not send any money to the cybercriminal. In addition, consider reporting the message as spam through your email.[13]

23. The other variation of this email provided:

Dear Valued Patient,

This message is to make you aware that Fred Hutchinson Cancer Center recently experienced a cybersecurity incident. We are close partners with Fred Hutch Cancer Center; Fred Hutch serves as UW Medicine's cancer program and we advance cancer research together through the Fred Hutch/University of Washington/Seattle Children's Cancer Consortium. As a result of our work with Fred Hutch, the cybersecurity incident experienced on Fred Hutch systems impacted data for some UW Medicine patients who have not been seen at Fred Hutch.

Some patients have received an email from the cyber-criminals and we are sorry if you received one. Unfortunately, this is a common tactic they use and law enforcement has been notified of these messages. If you receive a message demanding a ransom, do not pay it. Please report these messages to the FBI's Internet Crime Complaint Center at ic3.gov. Then block the sender and delete the

[13] *See* Email to Plaintiff Joel Guay from Defendant Fred Hutchinson Cancer Center attached hereto as **Exhibit A**.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

> message. In addition, you may consider reporting the message as spam through your email.
>
> Immediate action was taken to contain the impact, including contacting federal law enforcement, engaging a leading forensic security firm and proactively taking the Fred Hutch clinical network offline. A forensic team is continuing to assess the situation and Fred Hutch will directly contact any individuals whose information was involved.[14]

24. To date, Defendant has still failed to provide any notice of data breach letters to Plaintiffs and, on information and belief, Class Members. Indeed, the early December 2023 emails received by Plaintiffs are woefully inadequate and fail to provide any details about the Data Breach that would allow for Plaintiffs and Class Members to take action to protect themselves against the cybercriminals that stole their Personal Information.

25. While the emails provide little to no insight as to the Data Breach, Defendant's website provides that on November 19, 2023, Defendant "detected unauthorized activity on [its] clinical network."[15] Defendant surprisingly do not provide any further information but believe that "the criminal group responsible [for the Data Breach] is [located] outside the United States."[16]

26. Defendant claims that "the UW Medicine system was not impacted."[17] However, on information and belief, the Data Breach did indeed impact the broader UW Medicine system. This is because Defendant stated that "UW Medicine clinicians also provide care to patients at Fred Hutch and some services are provided across multiple Fred Hutch and UW Medicine locations."[18] On information and belief, Class Members were each contacted by Defendant as well and therefore their information was also involved in the Data Breach.

---

[14] *See* Emails to Plaintiffs Gary Holz and Gloria Moncrief from Defendant Fred Hutchinson Cancer Center attached hereto as **Exhibit B**.
[15] *See* https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html (last visited December 27, 2023).
[16] *Id.*
[17] *Id.*
[18] *Id.*

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

27. Moreover, Defendant readily admits that Class Members are "receiv[ing] threatening spam email" which is further evidence that the cybercriminal actors were able to access Defendant's systems and exfiltrate Plaintiffs' and Class Members' Personal Information.[19] Indeed, Defendant even warned that "[i]f the[se] message[s] demand[] ransom, **DO NOT PAY IT**" again illustrating the severity of the Data Breach and the fact that Plaintiffs' and Class Members' Personal Information was exfiltrated by, and is currently being used by, cybercriminals to further victimize Plaintiffs and Class Members.[20]

28. Worryingly, Class Members have begun to receive "threatening emails claiming names, Social Security numbers, medical history and other data of more than 800,000 patients had been compromised."[21]

29. To make matters even worse, Defendant delayed notifying Plaintiffs and Class Members until approximately a full month after the Data Breach and has failed to emphasize the severity of the Data Breach. Indeed, Defendant's *Update on Data Security Incident* fails to provide critical information including the types of Personal Information stolen in the Data Breach, and whether or not the cybercriminals were able to exfiltrate Plaintiffs' and Class Members' Personal Information. As explained in detail *infra*, the cybercriminals were able to exfiltrate Plaintiffs' and Class Members' Personal Information, including Social Security numbers and medical history information, as illustrated by the threatening ransom messages Class Members have been receiving.[22]

30. This substantial delay notifying Plaintiffs and Class Members, and Defendant's woefully inadequate and misleading warning to the public, deprived Plaintiffs and Class Members

---

[19] *Id.*
[20] *Id.*
[21] *See* ABC NEWS, *Some Seattle cancer center patients are receiving threatening emails after last month's data breach*, (Dec. 9, 2023) https://abc17news.com/ap-national/2023/12/09/some-seattle-cancer-center-patients-are-receiving-threatening-emails-after-last-months-data-breach/ (last visited December 27, 2023).
[22] *Id.*

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

of the opportunity to mitigate their injuries and risk of fraud and only further portrays Defendant's wholly inadequate data security and data breach notification practices.

31. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. Furthermore, upon information and belief, the putative class is well over one thousand members, as it includes Defendant's current and former patients.

32. Defendant failed in upholding its duties to Plaintiffs and Class Members when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Personal Information. As such, Defendant's negligence has caused widespread injury and monetary damages to Plaintiffs and Class Members.

33. Plaintiffs' and Class Members' sensitive Personal Information has been stolen, sold, and on information and belief, reviewed by cybercriminals.

34. Further, the Notice of Data Breach shows that Defendant cannot, or will not, determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and by whom it was stolen.

35. Defendant has done little to remedy the Data Breach. While Defendant has offered some Class Members basic credit monitoring, such offerings are wholly insufficient given the scope of the Data Breach and the type of Personal Information stolen.

The Effects of the Data Breach on Plaintiff Gary Holz

36. Defendant sent Plaintiff Holz an email stating that his Personal Information may have been exposed in the Data Breach on or around December 7, 2023.

37. Following the Data Breach, Plaintiff Holz experienced a substantial uptick in the number and frequency of spam calls and emails attempting to obtain further Personal Information from him.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

38. Plaintiff Holz made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Defendant; and dealing with unwanted spam emails and telephone calls.

39. Plaintiff Holz has spent a considerable amount of time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

40. Plaintiff Holz suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his Personal Information, a form of property that Defendant obtained from Plaintiff Holz; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

41. As a result of the Data Breach, Plaintiff Holz anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Holz is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

The Effect of the Data Breach on Joel Guay

42. Defendant sent Plaintiff Guay an email stating that his Personal Information may have been exposed in the Data Breach on or around December 7, 2023.

43. Plaintiff Guay made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Defendant; and dealing with unwanted spam emails and telephone calls.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

44. Plaintiff Guay has spent a considerable amount of time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

45. Plaintiff Guay suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his Personal Information, a form of property that Defendant obtained from Plaintiff Guay; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

46. As a result of the Data Breach, Plaintiff Guay anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Guay is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

The Effects of the Data Breach on Plaintiff Gloria Moncrief

47. Defendant sent Plaintiff Moncrief an email stating that her Personal Information may have been exposed in the Data Breach on or around December 15, 2023.

48. Following the Data Breach, Plaintiff Moncrief experienced a substantial uptick in the number and frequency of spam calls and emails attempting to obtain further Personal Information from her.

49. Plaintiff Moncrief made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Defendant; and dealing with unwanted spam emails and telephone calls.

50. Plaintiff Moncrief has spent a considerable amount of time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

51. Plaintiff Moncrief suffered actual injury from having her Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of her Personal Information, a form of property that Defendant obtained from Plaintiff Moncrief; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

52. As a result of the Data Breach, Plaintiff Moncrief anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Moncrief. As a result of the Data Breach, Plaintiff Moncrief is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

The Effects of the Data Breach on Plaintiff and Class Members

53. Plaintiffs' experiences in connection with the Data Breach are typical of those of the Class Members.

54. Given the sensitive nature of the Personal Information stolen in the Data Breach, hackers have the ability to commit identify theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

55. As a result of the Data Breach, Plaintiffs and Class Members will have to take a variety of steps to monitor for and safeguard against identity theft, and they are at a much greater risk of suffering such identity theft. In addition, these victims of the Data Breach are at a heightened risk of potentially devastating financial identity theft. As the Bureau of Justice Statistics reports, identity theft causes its victims out-of-pocket monetary losses and costs the nation's economy billions of dollars every year.[23]

56. Plaintiffs and Class Members have spent and will spend time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services,

[23] *See* U.S. Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), http://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited December 27, 2023).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

57. The Personal Information exposed in the Data Breach is highly coveted and valuable on underground or black markets. A cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web," exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; and (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

58. Consumers are injured every time their data is stolen and placed on the Dark Web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

59. Exposure of this information to the wrong people can have serious consequences. Identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2018-2020 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans and mortgages.[24] For some victims, this

[24] *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, https://www.idtheftcenter.org/publication/identity-theft-the-aftermath-study/ (last visited December 27, 2023).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

60. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[25]

61. The unauthorized disclosure of Social Security numbers can be particularly damaging because Social Security numbers cannot easily be replaced. To obtain a new number, a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until damage has been done. Furthermore, as the Social Security Administration warns:

> [A] new number probably won't solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other

[25] *See* FTC, *Combatting Identity Theft A Strategic Plan* (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited December 27, 2023).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

> personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security number, you shouldn't use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.[26]

56. According to the Attorney General of the United States, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[27] Indeed, as explained recently:

> The ubiquity of the SSN as an identifier makes it a primary target for both hackers and identity thieves. . . . When data breaches expose SSNs, thieves can use these numbers—usually combined with other pieces of data—to impersonate individuals and apply for loans, housing, utilities, or government benefits. Additionally, this information may be sold on the black market to other hackers.[28]

57. As the result of the Data Breach, Plaintiffs and Class Members are likely to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

d. lowered credit scores resulting from credit inquiries following fraudulent activities;

e. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data

---

[26] *See Identity Theft and Your Social Security Number* (July 2021), Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 27, 2023).
[27] *See Fact Sheet: The Work of the President's Identity Theft Task Force*, DOJ 06-636, 2006 WL 2679771 (Sep. 19, 2006).
[28] *See* Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 Duke L.J. 555, 564-65 (2018).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

> Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and
>
> f. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

58. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again, as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[29]

59. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[30]

60. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.

61. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

---

[29] *See* E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited December 27, 2023).

[30] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

62. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[32] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[33,34] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[35]

63. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information , which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

Defendant Failed to Comply with FTC Guidelines

64. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

---

[31] *See* U.S Government Accountability Office Report to Congressional Requesters, *Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited December 27, 2023).

[32] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

[33] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[34] https://datacoup.com/

[35] https://digi.me/what-is-digime/

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

65. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[36] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[37]

66. The FTC further recommends that companies not maintain personally identifiable information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

67. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[36] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last visited December 27, 2023).

[37] *Id*.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

68. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

69. Defendant failed to properly implement basic data security practices.

70. Defendant's failure to employ reasonable and appropriate measures to protect against and detect unauthorized access to patients' Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

71. Defendant was at all times fully aware of its obligation to protect the Personal Information of current and former patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

72. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Personal Information which they collect and maintain.

73. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

74. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

75. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

76. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

77. The Health Insurance Portability and Accountability Act ("HIPAA") requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

78. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of Personal Information. Safeguards must include physical, technical, and administrative components.

79. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Personal Information like the data Defendant left unguarded. The HHS subsequently

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

80. A data breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of private health information ("PHI") not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

81. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

V. CLASS ACTION ALLEGATIONS

82. Class Definition. Under Fed. R. Civ. P. 23, Plaintiffs bring this case as a class action against Defendant on behalf of the Class preliminarily defined as follows:

> All individuals in the United States whose Personal Information was compromised in the Data Breach disclosed by Defendant that occurred in or around November 2023 (the "Nationwide Class").

83. Excluded from the Class are the following: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any judge to whom this case is assigned, as well as his or her staff and immediate family.

84. In the alternative, and pursuant to Fed. R. Civ. P. 23, Plaintiffs bring this case as a class action against Defendant on behalf of a subclass preliminarily defined as follows:

> All individuals who reside in the state of Washington whose Personal Information was compromised in the Data Breach disclosed by Defendant that occurred in or around November 2023 (the "Washington Subclass").

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

85. Excluded from the Washington Subclass are the following: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any judge to whom this case is assigned, as well as his or her staff and immediate family.

86. The Nationwide Class and the Washington Subclass shall be collectively known as the "Class" unless otherwise specified.

87. Plaintiffs reserve the right to amend the Class definition.

88. Numerosity. Upon information and belief, the Class is so numerous that joinder of all members is impracticable. Reports suggest that the number of affected individuals may be as high as 800,000.[38] The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiffs only through the discovery process. The Class Members will be identifiable through information and records in Defendant's possession, custody, and control.

89. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all Class Members. These questions predominate over the questions affecting individual Class Members. These common legal and factual questions include, but are not limited to:

a. When Defendant learned of the Data Breach;

b. Whether cybercriminals obtained Class Members' Personal Information in the Data Breach;

c. Whether Defendant's response to the Data Breach was adequate;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information compromised in the Data Breach;

[38] *See* Kate Walters, *Hundreds of patients receive threatening emails after Fred Hutch cyberattack, KUOW* (Dec. 6, 2023), https://www.kuow.org/stories/hundreds-of-patients-receive-threatening-emails-after-fred-hutch-cyberattack (last visited December 27, 2023).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, industry standards, and/or its own promises and representations;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendant owed a duty to Class Members to safeguard their Personal Information;

h. Whether Defendant breached its duty to Class Members to safeguard their Personal Information;

i. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

j. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

k. Whether Defendant's conduct violated the FTCA, HIPAA, and/or the Consumer Protection Act invoked herein;

l. Whether Defendant's conduct was negligent;

m. Whether Defendant was unjustly enriched;

n. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

o. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

p. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

q. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

90. Typicality. All of Plaintiffs' claims are typical of the claims of Class Members. Upon information and belief, Plaintiffs and Class Members had their Personal Information compromised in the Data Breach. Plaintiffs' claims and damages are also typical of the Class because they resulted from Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiffs are entitled to is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

91. Adequacy. Plaintiffs are adequate class representatives because their interests do not materially or irreconcilably conflict with the interests of the Class Members they seek to represent, they retained counsel competent and highly experienced in complex class action litigation, and they intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of Class Members. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other Class Members.

92. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiffs and Class Members, a class action is the most superior. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for Class Members individually to effectively redress the wrongs done to them. Even if the Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Class Members can be readily identified and notified based on Defendant's records and databases.

VI. CAUSES OF ACTION

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

COUNT I
NEGLIGENCE
Claim of Relief for Plaintiffs and Class Members and Against Defendant

93. Plaintiffs incorporate by reference all foregoing factual allegations.

94. Defendant collected and transferred Personal Information from Plaintiffs and Class Members and had a corresponding duty to protect such information from unauthorized access.

95. Defendant failed to inform Plaintiffs and Class Members that its systems were inadequate to safeguard sensitive Personal Information and that transferring Personal Information could lead to cybercriminals gaining access to sensitive Personal Information.

96. The sensitive nature of the Personal Information and economic value of it to hackers necessitated security practices and procedures sufficient to prevent unauthorized access to the Personal Information.

97. Defendant failed to implement and maintain adequate security practices and procedures to prevent the Data Breach.

98. Defendant likewise failed to test, update, and patch (including curing known vulnerabilities) its systems as necessary.

99. It was reasonably foreseeable to Defendant that its failure to implement and maintain reasonable security procedures and practices would leave the sensitive Personal Information in its systems vulnerable to breach and could thus expose the owners of that information to harm.

100. Furthermore, given the known risk of major data breaches, including the 2021 breach of the Washington State Auditor's Office, Plaintiffs and Class Members are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their Personal Information stolen.

101. Defendant's duty of care arose as a result of its knowledge that individuals trusted Defendant to protect their confidential data that they provided to it. Only Defendant was in a

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

position to ensure that its own protocols were sufficient to protect against the harm to Plaintiffs and Class Members from a data breach of its own systems.

102. Defendant also had a duty to use reasonable care in protecting confidential data because it committed to comply with industry standards for the protection of Personal Information and committed to the public to protect the privacy of information the public provided Defendant.

103. Defendant knew, or should have known, of the vulnerabilities in its security practices and procedures, and the importance of adequate security to patients and the owners of sensitive data.

104. Plaintiffs and Class Members have suffered harm as a result of Defendant's negligence. These victims suffered diminished value of their sensitive Personal Information. Plaintiffs and Class Members also lost control over the Personal Information exposed, which subjected each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft, in addition to the time and expenses spent mitigating those injuries and preventing further injury.

COUNT II
NEGLIGENCE *PER SE*
Claim of Relief for Plaintiffs and Class Members and Against Defendant

105. Plaintiffs incorporate by reference all foregoing factual allegations.

106. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiffs and Class Members.

107. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect personal information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

108. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Class Members due to the valuable nature of the Personal Information at issue in this case—including Social Security numbers and medical history information.

109. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

110. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

111. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

112. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine how their Personal Information is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

placing freezes on credit reports; (vii) the continued risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information of current and former patients in their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

113. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information in its continued possession.

COUNT III
BREACH OF IMPLIED CONTRACT
Claim of Relief for Plaintiffs and Class Members and Against Defendant

114. Plaintiffs incorporate by reference all foregoing factual allegations.

115. Plaintiffs' and Class Members' Personal Information was provided to Defendant as part of medical services that Defendant provided to Plaintiffs and Class Members.

116. Plaintiffs and Class Members agreed to pay Defendant for medical care and services.

117. Defendant and the Plaintiffs and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiffs' and Class Members' Personal Information, whereby, Defendant was

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

obligated to take reasonable steps to secure and safeguard Plaintiffs' and Class Members' Personal Information.

118. Defendant had an implied duty of good faith to ensure that the Personal Information of Plaintiffs and Class Members in their possession was only used in accordance with its contractual obligations.

119. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' Personal Information and to comply with industry standards and applicable laws and regulations for the security of this information.

120. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiffs and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their Personal Information.

121. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' Personal Information, resulting in the Data Breach.

122. Defendant further breached the implied contract by providing untimely notification to Plaintiffs and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud. Indeed, Defendant noted that Class Members have been receiving threatening ransom demand emails as a result of the Data Breach (as detailed *supra*).

123. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

124. As a result of Defendant's conduct, Plaintiffs and Class Members did not receive the full benefit of the bargain.

125. Had Defendant disclosed that its data security was inadequate, neither the Plaintiffs or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

126. As a result of Data Breach, Plaintiffs and Class Members suffered actual damages resulting from the theft of their Personal Information, as well as the loss of control of their Personal Information, and remain at present risk of suffering additional damages.

127. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

128. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate lifetime credit monitoring to all Class Members.

COUNT IV
INVASION OF PRIVACY
Claim of Relief for Plaintiffs and Class Members and Against Defendant

129. Plaintiffs incorporate by reference all foregoing factual allegations.

130. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their highly sensitive and confidential Personal Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

131. Defendant owed a duty to their current and former patients, including Plaintiffs and Class Members, to keep this information confidential.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

132. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Personal Information is highly offensive to a reasonable person.

133. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and Class Members disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their Personal Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

134. The Data Breach constitutes an intentional interference with Plaintiffs' and Class Member's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

135. Defendant acted with a knowing state of mind when it permitted the Data Breach because they knew its information security practices were inadequate.

136. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and Class Members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

137. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

138. As a proximate result of Defendant's acts and omissions, the private and sensitive Personal Information of Plaintiffs and Class Members were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and Class Members to suffer damages (as detailed *supra*).

139. Furthermore, on information and belief, Plaintiffs' and Class Members' Personal Information has already been published—or will be published imminently—by cybercriminals on the dark web.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

140. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members since their Personal are still maintained by Defendant with its inadequate cybersecurity system and policies.

141. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Personal Information of Plaintiffs and Class Members.

142. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT V
UNJUST ENRICHMENT
Claim of Relief for Plaintiffs and Class Members and Against Defendant

143. Plaintiffs incorporate by reference all foregoing factual allegations.

144. This claim is pleaded in the alternative to the breach of implied contract claim.

145. Plaintiffs and Class Members conferred a benefit upon Defendant. Defendant benefitted from using its payment and Personal Information to provide medical services. Furthermore, Defendant benefitted from using their Personal Information to collect payment.

146. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members (or its third-party agents). Furthermore, Defendant benefited from receiving Plaintiffs' and Class Members' payment and Personal Information, as they were used to provide medical services.

147. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Personal Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

148. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information.

149. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

150. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class Members' Personal Information and payment because Defendant failed to adequately protect their Personal Information.

151. Plaintiffs and Class Members have no adequate remedy at law.

152. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

COUNT VI
VIOLATION OF WASHINGTON CONSUMER PROTECTION ACT (CPA) RCW 19.86.020, *et seq.*
Claim of Relief for Plaintiffs and Washington Subclass Members and Against Defendant

153. Plaintiffs incorporate by reference all foregoing factual allegations.

154. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

155. Defendant is a "person" as described in RWC 19.86.010(1).

156. Defendant engaged in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

157. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

158. In the course of conducting its businesses, Defendant committed "unfair or deceptive acts or practices" by, among other things, knowingly failing to ensure the safeguarding and protection of Plaintiffs' and Washington Subclass Members' Personal Information by the entities to whom it provided that Personal Information, and by violating the common law alleged herein in the process. Plaintiffs and Washington Subclass Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

159. Defendant also violated the CPA by concealing from Plaintiffs and Washington Subclass Members information regarding the unauthorized release and disclosure of their Personal Information. If Plaintiffs and Washington Subclass Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Personal Information and identities.

160. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

161. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

162. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CPA, Plaintiffs and Washington Subclass Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, among other things, (1) a present and imminent, immediate and the continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their Personal Information; (4) deprivation of the value of their Personal Information, for which there is a well-established national and international market; and/or (5) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

163. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves and Washington Subclass Members, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to ensure the safeguarding and protection of Plaintiffs' and Washington Subclass Members' Personal Information by the entities to whom they provide that Personal Information.

164. Plaintiffs, on behalf of themselves and Washington Subclass Members, also seek to recover actual damages sustained by each Washington Subclass Member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiffs, on behalf of

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

themselves and Washington Subclass Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Washington Subclass Members by three times the actual damages sustained, not to exceed $25,000.00 per Washington Subclass Member.

COUNT VII
VIOLATION OF WASHINGTON DATA BREACH DISCLOSURE LAW
RCW 19.255.005, *et seq.*
Claim of Relief for Plaintiffs and Washington Subclass Members and Against Defendant

165. Plaintiffs incorporate by reference all foregoing factual allegations.

166. Under RCW § 19.255.010(2), "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

167. Upon information and belief, this statute applies to Defendant because Defendant does not own nor license the Personal Information in question. Instead, the owners and/or licensees of the Personal Information are Plaintiffs and Washington Subclass Members.

168. Here, the Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant, leading to a "breach of the security of [Defendant's] systems," as defined by RCW § 19.255.010.

169. Defendant failed to disclose that the Personal Information, of Plaintiffs and Washington Subclass Members, that had been compromised "immediately" upon discovery, and thus unreasonably delayed informing Plaintiffs and Washington Subclass Members about the Data Breach.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

170. In fact, Defendant appears to have delayed notifying its current and former patients until December 2023, almost a full month after the Data Breach.

171. Thus, Defendant violated the Washington Data Breach Disclosure Law.

COUNT VIII
VIOLATION OF WASHINGTON UNIFORM HEALTH CARE INFORMATION ACT (UHCIA)
RCW 70.02.005, *et seq.*
Claim of Relief for Plaintiffs and Washington Subclass Members and Against Defendant

172. Plaintiffs incorporate by reference all foregoing factual allegations.

173. The UHCIA declares that:

r. "Health care information is personal and sensitive information that if improperly used or released may do significant harm to a patient's interests in privacy, health care, or other interests." § 70.02.005(1).

s. "In order to retain the full trust and confidence of patients, health care providers have an interest in assuring that health care information is not improperly disclosed and in having clear and certain rules for the disclosure of health care information." § 70.02.005(3).

t. "It is the public policy of this state that a patient's interest in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than health care providers." § 70.02.005(4).

174. Here, Defendant is a "health care provider" because Defendant is "licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession." § 70.02.010(19).

175. Under § 70.02.020, "a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization."

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

176. Here, Defendant violated UHCIA because Defendant, via the Data Breach, disclosed health care information of Plaintiffs and Washington Subclass Members to third parties without patient authorization.

VII. PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of Class Members, request that the Court enter judgment against Defendant as follows:

A. An order certifying the proposed Class pursuant to Fed. R. Civ. P. 23 and appointing Plaintiffs and their counsel to represent the Class;

B. An order awarding Plaintiffs and Class Members monetary relief, including actual damages and penalties;

C. An order awarding injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as necessary to protect the interests of Plaintiffs and Class Members, including, but not limited to, an order:

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its businesses in accordance with all applicable regulations, industry standards, and state or local laws;

iii. Requiring Defendant to delete, destroy, and purge the Personal Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. Requiring Defendant to implement and maintain comprehensive Information Security Programs designed to protect the confidentiality and integrity of the Personal Information of Plaintiffs and Class Members;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

v. Prohibiting Defendant from maintaining the Personal Information of Plaintiffs and Class Members on a cloud-based database;

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. Requiring Defendant to conduct regular database scanning and securing checks;

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Personal Information, as well as protecting the Personal Information of Plaintiffs and Class Members;

xii. Requiring Defendant to routinely and continually conduct internal training and education, and, on an annual basis, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

xiii. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting Personal Information;

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Personal Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. For a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

D. Ordering Defendant to pay for a lifetime of credit monitoring services for Plaintiffs and Class Members;

E. An award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law;

F. An award of attorney's fees, costs, and expenses, as permitted by law;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

G. An award of pre-judgment and post-judgment interest, as permitted by law;

H. Leave to amend this Complaint to conform to the evidence produced at trial; and

I. Such other and further relief as this Court may deem just and proper.

DATED this 28th day of December 2023.

Respectfully Submitted,

By: */s/ Timothy W. Emery*
By: */s/ Patrick B. Reddy*

TIMOTHY W. EMERY
WSBA No. 34078
PATRICK B. REDDY
WSBA No. 34092
EMERY REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
Phone: 206.442.9106
Fax: 206.441.9711
Email: *emeryt@emeryreddy.com*
Email: *reddyp@emeryreddy.com*

M. Anderson Berry*
Gregory Haroutunian*
Brandon P. Jack*
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: 916.239.4778
Fax: 916.924.1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Gary M. Klinger
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: 866.252.0878
gklinger@milberg.com

John J. Nelson*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Dr.
Beverly Hills, California 90212
Telephone: 858.209.6941
jnelson@milberg.com

**pro hac vice forthcoming*

Counsel for Plaintiffs and the Putative Class

Exhibit A

From: **Fred Hutchinson Cancer Center** no-rep y@fredhutch.org
Subject: Fred Hutch data secur ty nc dent
Date: December 7, 2023 at 14:36
To: Joe Guay [redacted]

View as Web page

Fred Hutch Cancer Center

December 7, 2023

Dear valued community,

We're writing to alert all current and former patients (including former Seattl Cancer Care Alliance patients) that Fred Hutchinson Cancer Center recentl experienced a cybersecurity incident. We took immediate action to contain impact, contacted federal law enforcement, engaged a leading forensic sec firm, and proactively took our clinical network offline.

All Fred Hutch clinics are open and actively serving patients.

Our patients' health and safety is our top priority. Our forensic team is conti to assess the data involved. We are working to complete the investigation a quickly as possible and will contact any individuals whose information was involved.

In the meantime, as a precautionary measure, we recommend you remain vigilant to protect against potential fraud and/or identity theft by, among othe things, reviewing your account statements and monitoring credit reports clo If you detect any suspicious activity on an account, you should promptly no the financial institution or company that maintains the account. You should promptly report any fraudulent activity or any suspected incidents of identity to appropriate law enforcement authorities, including the police and your sta attorney general, as well as the Federal Trade Commission ("FTC").

It is also common for cyber criminals to send threatening spam messages a demand money. If you receive suspicious or threatening phone calls or ema report these messages to the FBI's Internet Crime Complaint Center at ic3. Then block the sender, delete the message and do not send any money to cybercriminal. In addition, consider reporting the message as spam through email.

If you have additional questions, we have established a dedicated call cente support our patients, available at **888-983-0612**, Monday through Friday between 6 a.m. – 6 p.m. PT or Saturday and Sunday between 6 a.m. – 2 p. PT. You can also find information specific to this incident on our website at fredhutch.org/data-security.

Thank you for your patience and understanding.

Fred Hutchinson Cancer Center

Fred Hutchinson Cancer Center is an independent organization that serves as UW Medicine's cancer program.

UW Medici

Fred Hutch Cancer Center

825 Eastlake Ave E
PO Box 19023
Seattle, WA 98109
FredHutch.org
855.557.0555

Fred Hutchinson Cancer Center is a 501(c)(3) nonprofit organization.

Exhibit B

From: Gary Holz [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

----- Forwarded Message -----
From: "UW Medicine" <uwmedicine@info.uwmedicine.org>
To: [redacted]
Sent: Thu, Dec 7, 2023 at 4:49 PM
Subject: ^_Fred^_ ^_Hutch^_ Cybersecurity Incident

UW Medicine

Dear Valued Patient,

This message is to make you aware that Fred Hutchinson Cancer Center recently experienced a cybersecurity incident. We are close partners with Fred Hutch Cancer Center; Fred Hutch serves as UW Medicine's cancer program and we advance cancer research together through the Fred Hutch/University of Washington/Seattle Children's Cancer Consortium. As a result of our work with Fred Hutch, the cybersecurity incident experienced on Fred Hutch systems impacted data for some UW Medicine patients who have not been seen at Fred Hutch.

Some patients have received an email from the cyber-criminals and we are sorry if you received one. Unfortunately, this is a common tactic they use and law enforcement has been notified of these messages. If you receive a message

demanding a ransom, do not pay it. Please report these messages to the FBI's Internet Crime Complaint Center at ic3.gov. Then block the sender and delete the message. In addition, you may consider reporting the message as spam through your email.

Immediate action was taken to contain the impact, including contacting federal law enforcement, engaging a leading forensic security firm and proactively taking the Fred Hutch clinical network offline. A forensic team is continuing to assess the situation and Fred Hutch will directly contact any individuals whose information was involved.

Patient care is not interrupted; Fred Hutch, UW Medical Center, Harborview Medical Center and UW Medicine Primary Care clinics are open and serving patients.

If you have additional questions, Fred Hutch has established a dedicated call center to support patients: **888-983-0612**, available Monday through Friday between 6 a.m. – 6 p.m. PT and Saturday and Sunday between 6 a.m. – 2 p.m. PT. You can also find information specific to this incident at **fredhutch.org/data-security**.

Sincerely,

Timothy H. Dellit, MD
Chief Executive Officer, UW Medicine
Executive Vice President for Medical Affairs and
Paul G. Ramsey Endowed Dean of the School of Medicine,
University of Washington

From: Gloria Moncrief [redacted]

[redacted]

UW Medicine

Dear Valued Patient,

This message is to make you aware that Fred Hutchinson Cancer Center recently experienced a cybersecurity incident. We are close partners with Fred Hutch Cancer Center; Fred Hutch serves as UW Medicine's cancer program and we advance cancer research together through the Fred Hutch/University of Washington/Seattle Children's Cancer Consortium. As a result of our work with Fred Hutch, the cybersecurity incident experienced on Fred Hutch systems impacted data for some UW Medicine patients who have not been seen at Fred Hutch.

Some patients have received an email from the cyber-criminals and we are sorry if you received one. Unfortunately, this is a common tactic they use and law enforcement has been notified of these messages. If you receive a message demanding a ransom, do not pay it. Please report these messages to the FBI's Internet Crime Complaint Center at ic3.gov. Then block the sender and delete the message. In addition, you may consider reporting the message as spam through your email.

Immediate action was taken to contain the impact, including contacting federal law enforcement, engaging a leading forensic security firm and proactively taking the Fred Hutch clinical network offline. A forensic team is continuing to assess the situation and Fred Hutch will directly contact any individuals whose information was involved.

Patient care is not interrupted; Fred Hutch, UW Medical Center, Harborview Medical Center and UW Medicine Primary Care clinics are open and serving patients.

If you have additional questions, Fred Hutch has established a dedicated call center to support patients: 888-983-0612, available Monday through Friday between 6 a.m. – 6 p.m. PT and Saturday and Sunday between 6 a.m. – 2 p.m. PT. You can also find information specific to this incident at fredhutch.org/data-security.

Sincerely,

Timothy H. Dellit, MD
Chief Executive Officer, UW Medicine
Executive Vice President for Medical Affairs and
Paul G. Ramsey Endowed Dean of the School of Medicine,
University of Washington

The following is from a message in MyChart UW Medicine Fred Hutch Cancer Center

Fred Hutchinson Cancer Center Cybersecurity Incident

Fred Hutchinson Cancer Center recently experienced a cybersecurity incident. UW Medicine and Fred Hutch are close partners. As a result of our work with Fred Hutch, the cybersecurity incident experienced on Fred Hutch systems impacted data for some UW Medicine patients.

"Fred Hutch Cancer Center" "Cures Start Here"

Donate Now

Data Security Incident

Update on Data Security Incident

This page was last updated: Dec. 11, 2023

Fred Hutchinson Cancer Center recently detected unauthorized activity on limited parts of our clinical network. We immediately notified federal law enforcement and engaged a leading forensic security firm to investigate and contain the incident.

All Fred Hutch clinics are open and actively serving patients.

The safety, wellbeing, and personal information of our patients and employees is of the utmost importance to Fred Hutch. Our forensic team is continuing to conduct an assessment of the data accessed and we will provide further updates as we have them.

Additional information can be found in the FAQ below. For further questions, please contact our dedicated call center at 888.983.0612. You can also read the press release.

Collapse All

What exactly happened?

On November 19, 2023, we detected unauthorized activity on our clinical network. We immediately quarantined the servers, began investigating the incident and took steps to confirm the security of our systems. As a protective measure, we also proactively took our clinical network offline and implemented additional information technology security protocols. All Fred Hutch clinics are still open and actively serving patients while we continue to investigate.

Who did this?

Based on the information available, the criminal group responsible is outside the United States. Fred Hutch notified federal law enforcement and is providing information to support their investigation.

How did this happen?

Unfortunately, all organizations face cybersecurity risks and these kind of attacks have targeted multiple healthcare institutions in the past. Fred Hutch has experienced technology professionals and security tools in place that detected the unauthorized activity and effectively prevented additional damage. We are continuously updating and enhancing systems to prevent external parties from accessing information.

What is Fred Hutch doing to address the situation?

We immediately quarantined the impacted servers, notified federal law enforcement, and engaged a leading forensic security firm to investigate the incident and confirm the security of our systems. As a protective measure, we proactively took our clinical network offline and implemented additional information technology security protocols. We have also implemented additional defensive tools and increased monitoring to protect our data.

Was the UW Medicine system impacted?

At this time, it does not appear that the UW Medicine system was impacted.

I'm a UW Medicine patient – why does Fred Hutch have my data?

Since UW Medicine clinicians also provide care to patients at Fred Hutch and some services are provided across multiple Fred Hutch and UW Medicine locations, the patient data necessary to provide this care is shared across systems. The cybersecurity incident specifically involved Fred Hutch systems but those systems also had some UW Medicine patient data related to areas such as preventative and oncology care.

Was the Epic system impacted?

At this time, it does not appear that the Epic system was impacted.

Was study- or sponsor-related data impacted?

The Fred Hutch research network was not accessed. Our investigation is ongoing, but at this time we do not have reason to believe that study or sponsor data was involved.

Was MyChart impacted?

No, patients can still access MyChart.

Is my information secure?
Our investigation is ongoing and we are continuing to assess the data involved. We are working to complete the investigation as quickly as possible and will contact any individuals whose information was involved.
In the meantime, as a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely.
What should I do if I suspect fraud or identity theft?
If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that maintains the account. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to appropriate law enforcement authorities, including the police, as well as the Federal Trade Commission ("FTC"). You can also file a report with the FBI's Internet Crime Complaint Center at ic3.gov.
You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit https://www.identitytheft.gov/#/ or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
I have received a threatening spam email. What should I do?
We are sorry you're receiving these messages. Unfortunately, this is a common tactic threat actors use, and we have notified local and federal law enforcement of these messages. If the message demands a ransom, DO NOT PAY IT. Please report these messages to the FBI's Internet Crime Complaint Center at ic3.gov. Then block the sender and delete the message. In addition, you may consider reporting the message as spam through your email.
Are you offering credit monitoring for those impacted?
Our investigation is ongoing and we are continuing to assess the data involved. We are working to complete the investigation as quickly as possible and will contact any individuals whose information was involved, including any details about credit monitoring services.